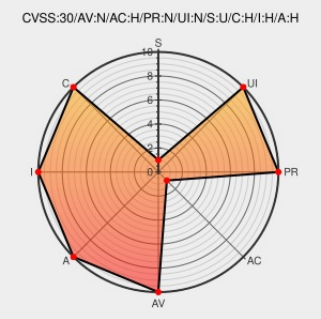
CVE-2016-9463

Published on: 03/27/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:18 PM UTC

CVE-2016-9463

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Nextcloud Server from Nextcloud contain the following vulnerability:

Nextcloud Server before 9.0.54 and 10.0.1 & ownCloud Server before 9.1.2, 9.0.6, and 8.2.9 suffer from SMB User Authentication Bypass. Nextcloud/ownCloud include an optional and not by default enabled SMB authentication component that allows authenticating users against an SMB server. This backend is implemented in a way that tries to connect to a SMB server and if that succeeded consider the user logged-in. The backend did not properly take into account SMB servers that have any kind of anonymous auth configured. This is the default on SMB servers nowadays and allows an unauthenticated attacker to gain access to an account without valid credentials. Note: The SMB backend is disabled by default and requires manual configuration in the Nextcloud/ownCloud config file. If you have not configured the SMB backend then you're not affected by this vulnerability.

CVE-2016-9463 has been assigned by support@hackerone.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Advisories – ownCloud	Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC owncloud.org/security/advisory/?id=oc-sa-2016-017
#148151 SMB User Authentication Bypass and Persistence - HackerOne	Exploit Third Party Advisory hackerone.com text/html	MISC hackerone.com/reports/148151
Merge pull request #2198 from owncloud/smb-auth-fix · owncloud/apps@5d47e7b · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/owncloud/apps/commit/5d47e7b52646cf79edadd78ce10c754290cbb732
Double verify the SMB response · nextcloud/apps@b85ace6 · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/nextcloud/apps/commit/b85ace6840b8a6704641086bc3b8eb8e81cb227
advisory – Nextcloud	Patch Vendor Advisory nextcloud.com text/html	MISC nextcloud.com/security/advisory/?id=nc-sa-2016-006
Operation OwnedCloud: Exploitation and Post-exploitation Persistence - Rhino Security Labs	Exploit Technical Description Third Party Advisory rhinosecuritylabs.com text/html	MISC rhinosecuritylabs.com/2016/10/operation-ownedcloud-exploitation-post-exploitation-persistence/
Double verify the SMB response · nextcloud/apps@decb91f · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/nextcloud/apps/commit/decb91fd31f4ffab191cbf09ce4e5c55c67a4087
[stable9] Merge pull request #2198 from owncloud/smb-auth-fix · owncloud/apps@16cbccf · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/owncloud/apps/commit/16cbccfc946c8711721fa684d78135ca1fb64791
[stable8.2] Merge pull request #2198 from owncloud/smb-auth-fix · owncloud/apps@a0e07b7 · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/owncloud/apps/commit/a0e07b7ddd5a5fd850a6e07f8457d05b76a300b3

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nextcloud	Nextcloud Server	All	All	All	All
Application	Nextcloud	Nextcloud Server	All	All	All	All
Application	Owncloud	Owncloud	All	All	All	All
Application	Owncloud	Owncloud	All	All	All	All

cpe:2.3:a:nextcloud:nextcloud_server:*:*:*:*:*:*:*:*:

cpe:2.3:a:nextcloud:nextcloud_server:*:*:*:*:*:*:*:*:

cpe:2.3:a:owncloud:owncloud:*:*:*:*:*:*:*:*:

cpe:2.3:a:owncloud:owncloud:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→